Czechoslovak Mathematical Journal, 53 (128) (2003), 769–775

INFINITE SIMPLE ZEROPOTENT PARAMEDIAL GROUPOIDS

Jung R. Cho, Pusan, and Tomáš Kepka, Praha

(Received November 9, 1999)

Abstract. The paper is an immediate continuation of [3], where one can find various notation and other useful details. In the present part, a full classification of infinite simple zeropotent paramedial groupoids is given.

Keywords: grupoid, simple, paramedial

MSC 2000: 20N02

1. Introduction

Let $\mathscr{T}$ be a transitive transformation semigroup on an infinite set G^* such that $\mathscr{T} = \langle f, g \rangle$, where f, g are projective transformations of G^*. Let $o \notin G^*$ and $G = G^* \cup \{o\}$. Now, define a multiplication on G as follows:

(a) $oo = o$;
(b) $ox = o = xo$ for every $x \in G^*$;
(c) $xy = o$ for all $x, y \in G^*$, $f(x) \neq g(y)$;
(d) $xy = f(x) = g(y)$ for all $x, y \in G^*$, $f(x) = g(y)$.

In this way, we get a groupoid $G = [\mathscr{T}, G^*, f, g, o]$.

1.1 Proposition.
(i) *G is balanced if and only if both f and g are permutations of G^*.*
(ii) *G is simple if and only if* $\ker(f) \cap \ker(g) = \mathrm{id}_{G^*}$.
(iii) *G is zeropotent if and only if $f(a) \neq g(a)$ for every $a \in G^*$.*

While working on this paper, the first author was supported by the Korea Research Foundation, Project No. 1998-015-D00008 and the second author by the Grant of the Czech Republic No. #201/96/0312 and by the institutional grant MSM113200007.

(iv) *If $f \neq g$, $f^2 = g^2$ and f, g are permutations of G^*, then G is zeropotent.*

(v) *G is paramedial if and only if f, g are permutations of G^* and $f^2 = g^2$.*

Proof. (i), (ii) and (iii)—see [5, Prop. 5.1].

(iv) We can proceed similarly as in the proof of [3, Prop. 1.1 (iii)].

(v) Assume that G is paramedial and let $a \in G^*$. Then there are $b, c, d \in G^*$ such that $f^2(a) = g^2(b)$, $f(a) = g(c)$ and $f(d) = g(b)$. Now, $f^2(a) = g^2(b) = ac \cdot db = bc \cdot da$, and so $f(b) = g(c)$, $f(d) = g(a)$ and $f^2(a) = g^2(b) = gf(d) = g^2(a)$. Thus $f^2 = g^2$. Further, let $x, y \in G^*$ be such that $f(x) = f(y)$. Then $x = f(u)$, $y = f(v)$ for suitable $u, v \in G^*$, $f^2(u) = f(x) = f(y) = f^2(v) = g^2(v)$ and $x = f(u) = f(v) = y$ by the preceding part of the proof. The rest is clear. $\square$

1.2 Lemma. *Suppose that both f and g are permutations of G^* and denote by $\mathscr{G}$ the permutation group generated by f, g. Then, for all $h \in \mathscr{G}$ and $a \in G^*$, there are $k_1, k_2, \in \mathscr{T}$ such that $hk_1(a) = a = k_2h(a)$.*

Proof. An immediate consequence of the transitivity of $\mathscr{T}$. $\square$

Let $\mathscr{B}_{\mathrm{zppm}}$ denote the class of ordered quadruples (A, B, a, b), where $A = \langle a, b\rangle$ is a group, $a \neq b$, $a^2 = b^2$, B is a corefree subgroup of A, the index $[A\colon B]$ is infinite and, for every $x \in A$, there exist elements r, s in the subsemigroup generated by a, b in A such that $xr, sx \in B$. Now, define an equivalence relation $\approx$ on $\mathscr{B}_{\mathrm{zppm}}$ by $(A_1, B_1, a_1, b_1) \approx (A_2, B_2, a_2, b_2)$ if and only if there is a (group) isomorphism $\lambda\colon A_1 \to A_2$ such that $\lambda(a_1) = a_2$, $\lambda(b_1) = b_2$ and the subgroups $\lambda(B_1)$, B_2 are conjugate in A_2.

Let $(A, B, a, b) \in \mathscr{B}_{\mathrm{zppm}}$, $A/B = \{xB;\ x \in A\}$. For every $x \in A$, the equality $\pi(x)(yB) = xyB$ defines a permutation $\pi(x)$ of A/B and we put $\Phi((A, B, a, b)) = [\pi(S), A/B, \pi(a), \pi(b), o]$, $o \notin A/B$, where S is the subsemigroup generated by a, b in A.

Let G be an infinite simple zeropotent paramedial groupoid (i.e., an infinite simple paramedial groupoid of type (II)—see [2]). Now, G is strongly balanced by [4, Theorem 2.1] and for every $a \in G^* = G \setminus \{o\}$ there exist uniquely determined elements $b, c \in G$ such that $f(a) = ab \neq o \neq ca = g(a)$. Furthermore, f, g are permutations of G^*, $f^2 = g^2$, $f \neq g$ and $\Psi(G) = (\mathscr{G}, \mathscr{H}, f, g) \in \mathscr{B}_{\mathrm{zppm}}$, where $\mathscr{G} = \langle f, g\rangle$ and $\mathscr{H} = \mathrm{Stab}_{\mathscr{G}}(\mathrm{u})$, $u \in G^*$.

1.3 Theorem. *There exists a one-to-one correspondence between isomorphism classes of infinite simple zeropotent paramedial groupoids and equivalence classes of quadruples from $\mathscr{B}_{\mathrm{zppm}}$. This correspondence is given by Φ and Ψ.*

Proof. Combine 1.1, 1.2 and [5, Theorem 6.1]. $\square$

2. Auxililary results on groups

Troughout this section, let A be an infinite non-commutative group such that $A = \langle a, b\rangle$, where $a^2 = b^2$. We put $A_1 = \langle a\rangle$, $c = a^{-1}b$, $C = \langle c\rangle$, $D = \langle a^2\rangle$ and $F = C \cap Z(A)$. Now, $A = \langle a, c\rangle$, $A' = \langle c^2\rangle \subseteq C$, $D \subseteq Z(A) = DF$ and $A = A_1C$. Since A is infinite, so is either A_1 or C.

2.1 Lemma.
(i) $A_1 \cap C = 1$ *and* $Z(A) = D \times F$.
(ii) *If* $F \neq 1$, *then* C *is finite of even order.*
(iii) $\operatorname{card}(A_1) \geqslant 2$ *and* $\operatorname{card}(C) \geqslant 3$.
(iv) $\operatorname{ord}(a) = \operatorname{ord}(b)$.
(v) *If* $\operatorname{ord}(a) = m$ *is finite, then* m *is even.*

Proof. $A_1 \cap C \subseteq F$. If $F \neq 1$, then C is finite of even order, A_1 is infinite and $A_1 \cap C = 1$. Further, if $a^{2k} = 1$ for some $k \geqslant 1$, then $b^{2k} = a^{2k} = 1$. On the other hand, if $a^{2k+1} = 1$ for some $k \geqslant 0$, then $1 = a^{2k+1} = b^{2k} \cdot a$, $a = b^{-2k}$ and $A = \langle a, b\rangle$ is abelian, a contradiction. $\square$

2.2 Lemma. *Let* B *be a corefree subgroup of* A. *Then* $B \cap C = 1 = B \cap D$, B *is isomorphic to a subgroup of* $A/C \cong A_1$ *and* B *is cyclic.*

Proof. Obvious. $\square$

2.3 Lemma. *Suppose that* A_1 *is finite of order* m *and let* B *be a non-trivial corefree subgroup of* A. *Then:*
(i) $m = 2m_2$, m_2 *odd.*
(ii) $B \cong \mathbb{Z}_2$ *and* $B = \langle a^{m_2}c^k\rangle$, $k \in \mathbb{Z}$.

Proof. We have $B = \langle a^\alpha c^\beta\rangle$, $1 \leqslant \alpha < m$ and $\beta \in \mathbb{Z}$. If α is even, then $(a^\alpha c^\beta)^m = a^{m\alpha}c^{m\beta} = c^{m\beta} \in B \cap C = 1$, $\beta = 0$ and $B \subseteq D$. However, then $B = 1$, a contradiction. Thus α is odd and $(a^\alpha c^\beta)^2 = a^{2\alpha} \in B \cap D = 1$. It follows that $m \mid 2\alpha$, and so $m = 2\alpha$, $\alpha = m_2$. $\square$

2.4 Lemma. *Suppose that* A_1 *is finite of order* $m = 2m_2$, m_2 *odd. For* $k \in \mathbb{Z}$, *let* $B_k = \langle a^{m_2}c^k\rangle$. *Then:*
(i) $B_k \cong \mathbb{Z}_2$ *is a corefree subgroup of* A.
(ii) *If* $l \in \mathbb{Z}$, *then* B_k, B_l *are conjugate in* A *iff* $k - l$ *is even.*

Proof. (i) Obvious.

(ii) If $\alpha \geqslant 0$ and $\beta \in \mathbb{Z}$, then $c^{-\beta}a^{-\alpha}a^{m_2}c^k a^\alpha c^\beta$ is equal to $a^{m_2}c^{k+2\beta}$ for α even and to $a^{m_2}c^{2\beta-k}$ for α odd. On the other hand, if $k - l = 2\gamma$, then $c^\gamma a^{m_2}a^k c^{-\gamma} = a^{m_2}c^{k-2\gamma} = a^{m_2}c^l$. $\square$

2.5 Lemma. *Suppose that A_1 is infinite and let B be a non-trivial corefree subgroup of A. Then:*

(i) *C is infinite.*

(ii) *$B = \langle a^k c^l \rangle$, $k, l \in \mathbb{Z}$, $0 \neq k$ even and $l \neq 0$.*

Proof. If k is odd, then $(a^k c^l) = a^{2k} \in B \cap D = 1$, and hence $k = 0$, $c^l \in B \cap C = 1$, a contradction. Thus k is even and, clearly, $k \neq 0 \neq l$. Finally, $(a^k c^l)^t = a^{tk} c^{lt}$ for every $t \in \mathbb{Z}$, $a^{tk} \in D \subseteq Z(A)$, and hence the order of c^l is infinite. □

2.6 Lemma. *Suppose that both A_1 and C are infinite. Then:*

(i) *Every non-identical element from A has infinte order.*

(ii) *If $k, l \in \mathbb{Z} \setminus \{0\}$, then $B_{k,l} = \langle a^k c^l \rangle$ is a corefree subgroup of A.*

(iii) *The subgroups B_{k_1,l_1} and B_{k_2,l_2} are conjugate in A iff $k_1 = k_2$ and $l_1 = \pm l_2$.*

Proof. Easy. □

Let S denote the subsemigroup generated in A by the elements a, b.

2.7 Lemma. $S = \{a^i;\ i \geqslant 1\} \cup \{a^i c^j;\ i \geqslant 2j - 1,\ j \geqslant 1\} \cup \{a^i c^{-j};\ i \geqslant 2j,\ j \geqslant 1\}$.

Proof. Easy. □

2.8 Corollary. *$S = A$ iff A_1 is of finite order.*

2.9 Lemma. *Suppose that both A_1 and C are infinite, $k, l \in \mathbb{Z} \setminus \{0\}$, k even and $B = B_{k,l}$ (see 2.6). The following conditions are equivalent:*

(i) *$S \cap xB \neq \emptyset$ for every $x \in A$.*

(ii) *$S \cap Bx \neq \emptyset$ for every $x \in A$.*

(iii) *Either $l > 0$ and $k > 2l$ or $l > 0$ and $k < -2l$ or $l < 0$ and $k < 2l$ or $l < 0$ and $k > -2l$.*

(iv) *$|2l| < |k|$.*

Proof. Let $\alpha, \beta \in \mathbb{Z}$ and $x = a^\alpha c^\beta$. According to 2.7, $s \cap xB \neq \emptyset$ iff there is $\gamma \in \mathbb{Z}$ such that at least one of the following three conditions is satisfied:

(1) $\gamma k \geqslant 1 - \alpha$ and $\gamma l = -\beta$;

(2) $\gamma(k - 2l) \geqslant 2\beta - \alpha - 1$ and $\gamma l \geqslant 1 - \beta$;

(3) $\gamma(k + 2l) \geqslant -2\beta - \alpha$ and $\gamma l \leqslant -\beta - 1$.

Assume $l > 0$ (the other case, $l < 0$, being similar). If $k > 2l$, then there exists $\gamma > 0$ such that (2) is true. If $k < -2l$, then (3) is true for some $\gamma < 0$.

Let $-2l \leqslant k \leqslant 2l$, so that $k-2l \leqslant 0 \leqslant k+2l$. Choose $\beta \in \mathbb{Z}$ such that $l \nmid \beta$ and $\alpha \in \mathbb{Z}$ such that $\alpha < 2\beta - 1 + ((\beta-1)(k-2l)/l)$ and $\alpha < -2/\beta + ((\beta+1)(k+2l)/l)$. Then, for any $\gamma \in \mathbb{Z}$, neither (1) nor (2) nor (3) is satisfied.

We have proved that the conditions (i) and (iv) are equivalent.

If α is even, then $xB = Bx$, $x = a^\alpha c^\beta$. Hence, assume that α is odd. Similarly as above, $S \cap Bx \neq \emptyset$ iff there is $\gamma \in \mathbb{Z}$ such that at least one of the following three conditions is satisfied:

(4) $\gamma k \geqslant 1-\alpha$ and $\gamma l = \beta$;

(5) $\gamma(k+2l) \geqslant 2\beta - \alpha - 1$ and $\gamma l \leqslant \beta - 1$;

(6) $\gamma(k-2l) \geqslant -2\beta - \alpha$ and $\gamma l \geqslant \beta + 1$.

Let $l > 0$ (the other case being similar). If $k > 2l$, then (6) is satisfied ($\gamma > 0$). If $k \geqslant -2l$, then (5) is satisfied ($\gamma < 0$). If $-2l \leqslant k \leqslant 2l$, choose $\beta \in \mathbb{Z}$ such that $l \nmid \beta$ and $\alpha \in \mathbb{Z}$ such that α is odd, $\alpha < 2\beta - 1 + ((1-\beta)(k+2l)/l)$ and $\alpha < -2\beta + ((-\beta-1)(k-2l)/l)$. Then, for any $\gamma \in \mathbb{Z}$, neither (4) nor (5) nor (6) is satisfied.

We have proved that (ii) is equivalent to (iv); this equivalence follows also from the fact that (i), (ii) are equivalent and the condition (iv) is not left-right asymmetric.

□

2.10 Proposition. *Let B be a subgroup of A. Then $(A, B, a, b) \in \mathscr{B}_{\mathrm{zppm}}$ if and only if at least one of the following three cases takes place:*

(1) *A_1 is of finite order and $B = 1$;*

(2) *A_1 is of finite order $2m_2$, m_2 odd, and $B = B_k$ (see 2.4);*

(3) *both A_1 and C are infinite and $B = B_{k,l}$, where $|2l| < |k|$ (see 2.6 and 2.9).*

Proof. Use the preceding lemmas. □

2.11 Lemma. *Let $\widetilde{a}, \widetilde{b} \in A$ such that $A = \langle \widetilde{a}, \widetilde{b} \rangle$ and $\widetilde{a}^2 = \widetilde{b}^2$. Then:*

(i) $\mathrm{ord}(a) = \mathrm{ord}(b) = \mathrm{ord}(\widetilde{a}) = \mathrm{ord}(\widetilde{b})$.

(ii) $\mathrm{ord}(c) = \mathrm{ord}(\widetilde{c})$, *where $\widetilde{c} = \widetilde{a}\widetilde{b}$.*

Proof. First, let $\mathrm{ord}(a) = \mathrm{ord}(b) = m$ be finite, m even (see 2.1). Then $\mathrm{ord}(c)$ is infinite, $Z(A) = D = \langle a^2 \rangle$, $\mathrm{card}(Z(A)) = m/2$, $\widetilde{D} \subseteq Z(A)$, and hence $\mathrm{ord}(\widetilde{a}) = \mathrm{ord}(\widetilde{b}) = \widetilde{m}$ is finite, $m/2 = \mathrm{card}(Z(A)) = \widetilde{m}/2$, $m = \widetilde{m}$ and $\mathrm{ord}(\widetilde{c})$ is infinite.

Next, let $\mathrm{ord}(c) = n$ be finite. Then $n \geqslant 3$, A' is finite, and so $\mathrm{ord}(\widetilde{c}) = \widetilde{n} \geqslant 3$ is also finite and $\mathrm{ord}(c^2) = \mathrm{card}(A') = \mathrm{ord}(\widetilde{c}^2)$. Consequently, $n = \widetilde{n}$, provided that both n and $\widetilde{n}$ are odd. Assume, finally, n to be even. Then $1 \neq c^{n/2} \in Z(A) = D \times F$, so that $\widetilde{F} \neq 1$, $\widetilde{n}$ is even and $n/2 = \mathrm{ord}(c^2) = \mathrm{ord}(\widetilde{c}^2) = \widetilde{n}/2$. Thus $n = \widetilde{n}$. □

3. Main results

3.1 Let $m \geqslant 2$ be even and $A = A(m, \infty, 1) = \mathbb{Z}_m \times \mathbb{Z}$. Define a multiplication on A by $(\alpha, \beta)(\gamma, \delta) = (\alpha + \gamma, (-1)^\gamma \beta + \delta)$. Then A becomes a group, $A = \langle a, b\rangle$, $a = (1, 0)$, $b = (1, 1)$, $a^2 = b^2$, $\operatorname{ord}(a) = m$ and $\operatorname{ord}(a^{-1}b)$ is infinite.

3.2 Proposition. *Let $m \geqslant 2$ be even.*

(i) *The group $A(m, \infty, 1)$ is given by two generators u, v and by the relations $u^2 = v^2$, $u^m = 1$.*

(ii) *If A is a group such that $A = \langle a, b\rangle$, $a^2 = b^2$, $\operatorname{ord}(a) = m$ and $\operatorname{ord}(a^{-1}b)$ infinite, then there exists an isomorphism $f\colon A(m, \infty, 1) \to A$ such that $f((1, 0)) = a$ and $f((1, 1)) = b$.*

3.3 Let $n \geqslant 3$ and $A = A(\infty, n, 2) = \mathbb{Z} \times \mathbb{Z}_n$. Define a multiplication on A by $(\alpha, \beta)(\gamma, \delta) = (\alpha + \gamma, (-1)^\gamma \beta + \delta$. Then A becomes a group, $A = \langle a, b\rangle$, $a = (1, 0)$, $b = (1, 1)$, $a^2 = b^2$, $\operatorname{ord}(a)$ is infinite and $\operatorname{ord}(a^{-1}b) = n$.

3.4 Proposition. *Let $n \geqslant 3$.*

(i) *The group $A(\infty, n, 2)$ is given by two generators u, v and by the relations $u^2 = v^2$, $(u^{-1}v)^n = 1$.*

(ii) *If A is a group such that $a^2 = b^2$ and $\operatorname{ord}(a^{-1}b) = n$, $\operatorname{ord}(a)$ infinite, then there exist an isomorphism $f\colon A(\infty, n, 2) \to A$ such that $f((1, 0)) = a$ and $f((1, 1)) = b$.*

3.5 Put $A = A(\infty, \infty, 3) = \mathbb{Z} \times \mathbb{Z}$ and define a multiplication on A by $(\alpha, \beta)(\gamma, \delta) = (\alpha + \gamma, (-1^\gamma \beta + \delta)$. Then A becomes a group, $A = \langle a, b\rangle$, $a^2 = b^2$, $a = (1, 0)$, $b = (1, 1)$ and the elements a, b, $a^{-1}b$ possess infinite order.

3.6 Proposition.

(i) *The group $A(\infty, \infty, 3)$ is given by two generators u, v and by the relation $u^2 = v^2$.*

(ii) *If A is a group such that $A = \langle a, b\rangle$, $a^2 = b^2$ and the orders $\operatorname{ord}(a)$, $\operatorname{ord}(a^{-1}b)$ are infinite, then there exists an isomorphism $f\colon A(\infty, \infty, 3) \to A$ such that $f((1, 0)) = a$ and $f((1, 1)) = b$.*

3.7 Proposition.

(i) $A(m, \infty, 1) \cong A(\widetilde{m}, \infty, 1)$ *iff* $m = \widetilde{m}$.

(ii) $A(\infty, n, 2) \cong A(\infty, \widetilde{n}, 2)$ *iff* $n = \widetilde{n}$.

(iii) $A(m, \infty, 1) \ncong A(\infty, n, 2) \ncong A(\infty, \infty, 3) \ncong A(m, \infty, 1)$.

P r o o f. We have $\operatorname{card}(Z(A(m, \infty, 1))) = m/2$ and $A(m, \infty, 1)'$ is infinite. Further, $\operatorname{card}(A(\infty, n, 2)') = n$ for n odd and $n/2$ for n even and $Z(A(\infty, n, 2))$ is infinite. $\square$

3.8 Proposition. *Let A be an infinite non-abelian group such that $A = \langle a, b\rangle = \langle \widetilde{a}, \widetilde{b}\rangle$, where $a^2 = b^2$ and $\widetilde{a}^2 = \widetilde{b}^2$. Then there exists an automorphism f of A such that $f(a) = \widetilde{a}$ and $f(b) = \widetilde{b}$.*

P r o o f. Use the preceding results. □

3.9 Proposition. *Let A be an infinite abelian group such that $A = \langle a, b\rangle$, where $a \neq b$ and $a^2 = b^2$. Then $1 \notin S$, where S denotes the subsemigroup generated by a, b in A.*

P r o o f. Easy. □

3.10 Put

$$\alpha_m = (A(m,\infty,1), \{(0,0)\}, (1,0), (1,1)),\ m \geqslant 2,\ 2 \mid m;$$
$$\beta_{n,0} = (A(n,\infty,1), \{(n/2,0), (0,0)\}, (1,0), (1,1));$$
$$\beta_{n,l} = (A(n,\infty,1), \{(n/2,1), (0,0)\}, (1,0), (1,1)),\ n \geqslant 2,\ 2 \mid n,\ 4 \nmid n;$$
$$\gamma_{k,l} = (A(\infty,\infty,3), \{(rk, rl);\ r \in \mathbb{Z}\}, (1,0), (1,1)),\ k \neq 0,\ 2 \mid k,\ l > 0,\ 2l < |k|.$$

According to the preceding results, these ordered quadruples are all in $\mathscr{B}_{\mathrm{zppm}}$, they are pair-wise non-equivalent and they form a set of representatives of the equivalence classes. Now, by 1.3, we have the following

3.11 Theorem. *The (pair-wise non-isomorphic) groupoids $\Phi(\alpha_m)$, $\Phi(\beta_{n,0})$, $\Phi(\beta_{n,1})$, $\Phi(\gamma_{k,l})$ (see* 3.10*) are (up to isomorphism) the only infinite simple zeropotent paramedial groupoids.*

3.12 Corollary. *Every simple zeropotent paramedial groupoid is countable and, up to isomorphism, there exist only countably many such groupoids.*

References

[1] *J. R. Cho, J. Ježek and T. Kepka*: Paramedial groupoids. Czechoslovak Math. J. *49* (1999), 277–290.
[2] *J. R. Cho, J. Ježek and T. Kepka*: Simple paramedial groupoids. Czechoslovak Math. J. *49* (1999), 391–399.
[3] *J. R. Cho, J. Ježek and T. Kepka*: Finite simple zeropotent paramedial groupoids. Czechoslovak Math. J. *52* (2002), 41–53.
[4] *R. El Bashir, J. Ježek and T. Kepka*: Simple zeropotent paramedial groupoids are balanced. Czechoslovak Math. J. *50* (2000), 397–399.
[5] *T. Kepka and P. Němec*: Simple balanced grupoids. Acta Univ. Palackianae Olomoucensis, Fac. rer. mat., Mathematica *35* (1996), 53–60.

Authors' addresses: J. R. Cho, Department of Mathematics, Pusan National University, Kumjung, Pusan 609-735, Republic of Korea, e-mail: `jungcho@hyowon.cc.pusan.ac.kr`; T. Kepka, Department of Algebra, Charles University, Sokolovská 83, 186 00 Praha 8, Czech Republic, e-mail: `kepka@karlin.mff.cuni.cz`.